

STABILIZATION BOUNDS FOR LINEAR FINITE DYNAMICAL SYSTEMS

BJÖRN LINDENBERG

ABSTRACT. A common problem to all applications of linear finite dynamical systems is analyzing the dynamics without enumerating every possible state transition. Of particular interest is the long term dynamical behaviour. In this paper, we study the number of iterations needed for a system to settle on a fixed set of elements. As our main result, we present two upper bounds on iterations needed, and each one may be readily applied to a fixed point system test. The bounds are based on submodule properties of iterated images and reduced systems modulo a prime. We also provide examples where our bounds are optimal.

1. INTRODUCTION

A *finite dynamical system* is an ordered pair (X, f) , which consists of a finite set X together with an iterating function f over X . That is, elements of X evolve by repeated application of f . Thus the study of a finite dynamical system is a study of sequences of the form

$$(1) \quad (x, f(x), f^2(x), \dots),$$

where f is called the *defining function*. In mathematical modelling, finite dynamical systems emerge in many different areas. Applications can be found in, for example, computational physics, electrical engineering, artificial intelligence, gene regulatory networks and cellular automata [HT05; CRLP05; CRJL06; BCRO07]. Hence, f often represents *state transitions* or the *passing of time*.

In this context, a *linear finite dynamical system* (M, f) is a system where f is a linear map and M is a *finite R -module*. That is, M is a generalized vector space with scalars in a finite commutative ring R , and is generated by a finite set of *base elements*. Therefore, f can be represented by a matrix A over R , which describes the mapping of the base elements.

An important problem in applications of finite dynamical systems, is the determination of long term behaviour without enumeration of all possible state transitions. The size of the underlying set X may lead to iteration over all elements being computationally intractable. As an example, a finite dynamical system in the form of a Boolean modeling framework is demonstrated in [LS04]. There the framework models a gene regulatory network of 60 nodes, such that $|X| = 2^{60}$. Other frameworks for gene regulatory networks may have more than two states for each node, leading to a further increase in the size of the underlying set [BCRO07].

When a linear finite dynamical system is given by (\mathbb{Z}_p^m, A) , where p is prime, the properties and long term behaviour is well understood [BCRO07; CRLP05; HT05]. Although when dealing with more general linear systems (\mathbb{Z}_n^m, A) , one faces difficulties due to the lack of unique factorization [XZ09; Den15].

1.1. Fixed Point Systems. Let (X, f) be a finite dynamical system and consider an iterated sequence of the form given in (1). It is possible that after a certain number of iterations we reach a *fixed point* x_0 , such that $f(x_0) = x_0$. If every element in X eventually iterates to a fixed point, not necessarily unique, then the system is called a *fixed point system*. Otherwise elements of X will eventually converge within a subset of X , which consists of fixed points and *cycles*, where cycles are closed iteration loops of more than one element. An extensive study of cycles of linear finite dynamical systems can be found in [Den15].

A *fixed point system criterion* for (\mathbb{F}_q^n, A) , where \mathbb{F}_q is the finite field with q elements, is given by Bollman *et al.* in [BCRO07]. It is based on the *minimal polynomial* of A , i.e., the polynomial of least degree in $\mathbb{F}_q[x]$ which annihilates A . As an alternative, G. Xu and Y.M. Zou presented another fixed point system criterion in [XZ09]. Given (R^m, A) , where R is a finite commutative ring, they showed that if the size of R is a composite integer n , then the system is fixed point system if and only if

$$(2) \quad A^{k+1} = A^k,$$

where $k = \lceil m \log_2(n) \rceil$. Thus the integer k is a derived bound on the number of iterations needed for the system to stabilize, and the criterion in (2) provides an efficient way of determining if the system exhibits long term *steady state* behaviour.

That every linear finite dynamical system eventually settles on fixed points and cycles is stated in *Fitting's Lemma*, see Theorem 2.2. In the spirit of [HT05] we define the *height* of a system as the minimum number of iterations needed for the system to settle. It is easy to show that the bound k in (2) can be replaced by any upper bound on the system height, generating an alternative fixed point system criterion. Thus, assuming a composite integer n for the size of the ring, one could ask the question of how close $\lceil m \log_2(n) \rceil$ is to the actual system height, and if there is significant improvements to be found.

In this paper we give sharper height bounds. We also provide examples where these bounds are optimal. Issues concerning implementation of our results and possible performance advantages is also addressed.

We proceed to discuss our main results in more detail.

1.2. Main Results. We present theorems which are height bounds for a linear finite dynamical system of the form (\mathbb{Z}_n^m, f) . As such they may be readily applied to a fixed point convergence test found in [XZ09, Section 3]. The main results come in two varieties. One is independent of the defining function, and the other is based on the structure of smaller reduced systems. In addition we will see examples and numerical applications of the main theorems.

Theorem A. (A Function Independent Bound). *Let (\mathbb{Z}_n^m, f) be a linear finite dynamical system, and let s be the system height. If the prime factorization of n is $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\omega^{\alpha_\omega}$, then the height is bounded as*

$$s \leq m \cdot \max \{ \alpha_1, \alpha_2, \dots, \alpha_\omega \},$$

where $\max \{ \alpha_1, \alpha_2, \dots, \alpha_\omega \}$ is the largest prime factor exponent.

The function independent bound $m\alpha_{\max}$ of Theorem A, where α_{\max} is the largest prime factor exponent of n , may be precalculated for any endomorphism given a certain module. Its proof relies on submodule properties of iterated images and reduced systems derived from the *primary decomposition* of the underlying ring.

Theorem B. (A Function Dependent Bound). *Let (\mathbb{Z}_n^m, f) be a finite dynamical system with a defining matrix A over \mathbb{Z}_n , and let s be the system height. If the*

prime factorization of n is $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\omega^{\alpha_\omega}$, then the height is bounded as

$$s \leq \max \{ \alpha_1 s_1, \alpha_2 s_2, \dots, \alpha_\omega s_\omega \},$$

where each s_i is the height of the reduced system $(\mathbb{Z}_{p_i}^m, A \bmod p_i)$, $i = 1, 2, \dots, \omega$.

The proof of [Theorem B](#) is based upon properties derived from *reduced* systems involving factor modules of prime powered orders.

The function dependent bound is the sharpest bound of this paper. When implementing [Theorem B](#) one needs to find the height of systems of the form (\mathbb{Z}_p^m, f) , where \mathbb{Z}_p^m is a vector space. Therefore one possible algorithm is as follows: For each distinct prime factor p of n calculate the product of the exponent of p and the height of $(\mathbb{Z}_p^m, A \bmod p)$. The height is found by checking the rank of successive powers of $A \bmod p$. The largest such product h_{\max} is then used in the fixed point convergence test. Although this naive implementation may require large scale linear finite dynamical systems to be effective, there is room for improvements concerning algorithms implementing it. The naive complexity for rank calculations and matrix multiplications is $O(m^3)$, although faster methods exist, see [\[VZGG13\]](#). Thus, the worst case complexity of the naive algorithm is on par with the function independent bounds, whose algorithms execute pure matrix multiplications.

In practice for smaller systems, the bound of [Theorem A](#) will be fast and efficient enough to outweigh any possible improvements gained by [Theorem B](#). However given an application of a large scale linear finite dynamical system we know that the true height is bounded by a product of an exponent and the height of some subsystem over a field. Thus the probability of the true height being significantly less than the exponent times the dimension of the matrix grows both with the prime of this subsystem and the dimension, see [\[LT94\]](#). Therefore any sufficient implementation of [Theorem B](#) will with high probability yield a performance advantage concerning fixed point system tests on these large scale systems.

1.3. Examples and Numerical Comparisons.

Example 1.1. With a system of the form $(\mathbb{Z}_{210}^{16}, f)$ we have $m = 16$ and $210 = 2^1 3^1 5^1 7^1$, thus by [Theorem A](#) the system height cannot be larger than $16 \cdot 1 = 16$.

Consider instead a system of the form (\mathbb{Z}_{1960}^4, f) . We have $m = 4$ and $1960 = 2^3 5^1 7^2$, yielding a maximal exponent of 3, as such the system height is less than or equal to $4 \cdot 3 = 12$. \diamond

Remark 1.1. [Theorem A](#) gives an upper bound that is only dependent on the prime factor exponents. A system of the form (\mathbb{Z}_6^3, f_1) has a height less than or equal to 3, since $6 = 2^1 3^1$ and $3 \cdot 1 = 3$. The same bound applies to a system of the form $(\mathbb{Z}_{400827403}^3, f_2)$. Here we have the prime factorization

$$400827403 = 10333^1 38791^1,$$

thus in spite of $\mathbb{Z}_{400827403}^3$ being a set many orders of magnitude larger than \mathbb{Z}_6^3 , the system will settle on cycles within three iterations. \spadesuit

Example 1.2. Let $(\mathbb{Z}_{27720}^4, A)$ be a linear finite dynamical system, with a defining matrix

$$A = \begin{pmatrix} 17453 & 19126 & 430 & 13601 \\ 3116 & 18264 & 19275 & 26452 \\ 22825 & 2401 & 22534 & 173 \\ 4496 & 13083 & 3885 & 12974 \end{pmatrix},$$

over \mathbb{Z}_{27720} . The prime factorization of 27720 is $2^3 3^2 5^1 7^1 11^1$. For each distinct prime p , we find the height of $(\mathbb{Z}_p^4, A \bmod p)$ and multiply it with the corresponding exponent. This leads to a set of products

$$\{3 \cdot 3, 2 \cdot 2, 1 \cdot 0, 1 \cdot 1, 1 \cdot 0\} = \{9, 4, 0, 1, 0\},$$

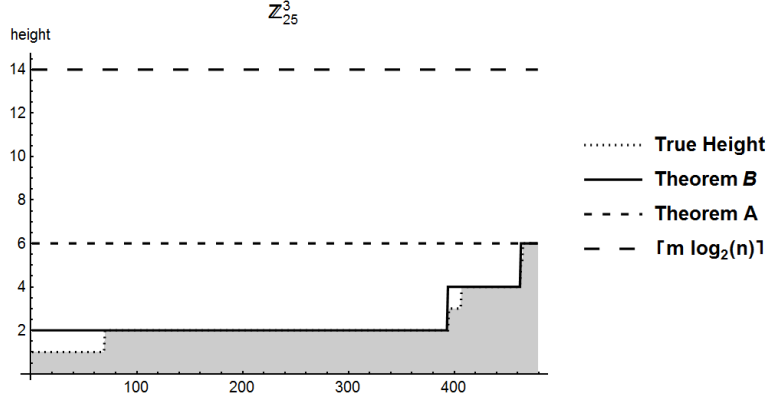


FIGURE 1. A number of sampled linear systems (\mathbb{Z}_{25}^3, f) for a bound comparison. Here [Theorem A](#) demonstrates that it is a least upper bound over all endomorphisms, and [Theorem B](#) follows closely the actual height.

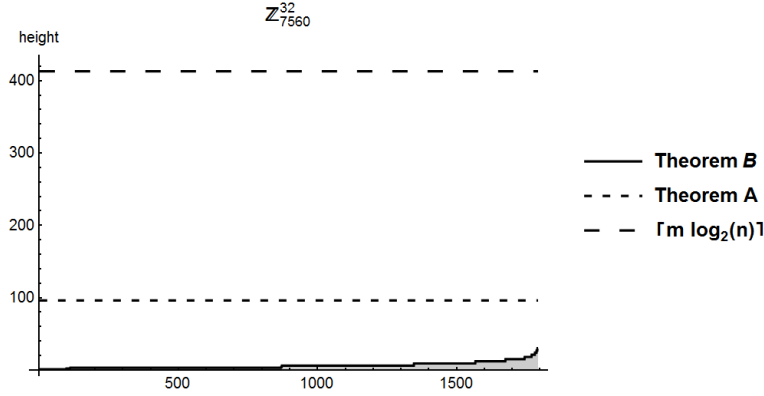


FIGURE 2. A number of sampled linear systems $(\mathbb{Z}_{7560}^{32}, f)$ for a bound comparison.

and according to [Theorem B](#), the system height is less than or equal to 9. \diamond

Example 1.3 (Sampled Height Bounds). In [Figure 1](#) height bounds are calculated for a number of sampled non-invertible matrices, and for reference the true height is included, which the data is sorted by. As can be seen, [Theorem B](#) follows closely the actual height of the systems, and [Theorem A](#) provides a least upper bound concerning all endomorphisms. [Figure 2](#) shows bounds for systems over a larger module. Here the number of distinct prime factors and base elements has increased compared to the former figure, which leads to relatively larger differences between the bounds. The figure shows that the function independent bounds may vastly overshoot the actual height of a system, where the height will be some integer less than or equal to the function dependent bound of [Theorem B](#). In both figures the function independent bound $\lceil m \log_2(n) \rceil$ derived in [\[XZ09\]](#) is added for comparison. \diamond

1.4. Organization and Strategy. We will follow the framework laid out in [\[HT05; BCRO07; Den15\]](#) and start with some basic notions concerning vertices in the associated state space and structural properties of product systems in [§ 2](#).

After the preliminaries, the proofs will be presented in [§ 3](#) and [§ 4](#). First a small addition to the train of thought used by Xu and Zou in [\[XZ09, Theorem 2.1\]](#). Iterated images of any linear map yields a descending chain of submodules, hence

the minimum number of iterations is bounded by the maximum chain length over all functions. This produces an intermediary bound in [Lemma 3.1](#), which involves $\Omega(n)$, the number of prime factors of n counting multiplicity. Furthermore the main theorems are partially a consequence of [Lemma 3.2](#), which equates the number of iterations needed for stabilization to that of subsystems arising from the primary decomposition of the underlying ring.

In § 4 we will derive properties of systems of the form $(\mathbb{Z}_{p^r}^m, f)$. This is done by looking at smaller reduced systems $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$ and $(\langle p \rangle^m, f)$, where \bar{f} is a function *induced* by the natural homomorphism from the module to its factor module. This will lead us to a bound when $M = \mathbb{Z}_{p^r}^m$ in [Lemma 4.6](#), which combined with [Lemma 3.2](#) proves [Theorem B](#): A function dependent bound when $M = \mathbb{Z}_n^m$.

ACKNOWLEDGEMENTS

I would like to thank Karl-Olof Lindahl and Per-Anders Svensson at Linnæus University for productive discussions, pointers to literature, and for corrections and improvements of earlier drafts of this paper.

2. PRELIMINARIES

In a finite dynamical system (X, f) every element is a vertex in the associated directed graph \mathcal{G}_f , called the *state space*, whose edges are given by the ordered pairs $\{(x, f(x)) \mid x \in X\}$. We hereby define two different instances of vertices.

Definition 2.1. Let (X, f) be a finite dynamical system with an associated state space \mathcal{G}_f . A *cycle vertex* is an element x_0 in X , such that $f^l(x_0) = x_0$ for some positive integer l , i.e., there exists a path from x_0 to itself in \mathcal{G}_f . The smallest such integer is called the *period* of x_0 . Furthermore, when cycle vertices are of period 1 they are called *fixed points*.

Definition 2.2. Let (X, f) be a finite dynamical system with an associated state space \mathcal{G}_f . A *leaf vertex* is an element y in X , such that y is a leaf in the associated state graph \mathcal{G}_f , i.e., the equation $f(x) = y$ has no solution.

Of special interest to us is the subgraph of \mathcal{G}_f consisting of only cycle vertices and their internal edges. When an element reaches a cycle vertex during iteration, the future iterated images will remain as cycle vertices. This is an immediate consequence of [Definition 2.1](#), i.e., if x_0 is a cycle vertex then $f^k(x_0)$ is a cycle vertex of the same period for all nonnegative integers k .

Thus given a finite dynamical system (X, f) and an element x in X , one could ask the questions: How many iterations does it take for x to reach a cycle vertex in the associated state space? How many iterations does it take to have a guaranteed cycle vertex regardless of starting element? These quantities are defined as follows.

Definition 2.3. Let (X, f) be a finite dynamical system and let x be an element in X . The number of iterations it takes for x to reach a cycle vertex during iteration is called the *height* of x , and is denoted $h(x)$.

Definition 2.4. Let (X, f) be a finite dynamical system. The *system height* s , defined by

$$s = \max_{x \in X} \{h(x)\},$$

is the largest possible height of all $x \in X$.

When furnishing the set \mathbb{Z}_n^m as a \mathbb{Z}_n -module and choosing any $m \times m$ matrix A over \mathbb{Z}_n , we get a linear finite dynamical system (\mathbb{Z}_n^m, f) , where f is a \mathbb{Z}_n -endomorphism defined by A . We now state a theorem which shows its *primary decomposition* in

the form of factor systems. The isomorphism ultimately has its root in the Chinese Remainder Theorem, and the primary decomposition of the underlying ring.

Theorem 2.1 ([Den15]). *Let (\mathbb{Z}_n^m, A) be a linear finite dynamical system with a defining $m \times m$ matrix A over \mathbb{Z}_n . If the prime factorization of n is given by*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\omega^{\alpha_\omega},$$

then (\mathbb{Z}_n^m, A) is isomorphic to

$$\prod_{k=1}^{\omega} (\mathbb{Z}_{p_k^{\alpha_k}}^m, A \bmod p_k^{\alpha_k}),$$

a product of linear finite dynamical systems.

Given a system of the form (\mathbb{Z}_p^m, f) , where p is prime, there is a natural reduction defined by the projective homomorphism to the quotient module $\mathbb{Z}_p^m / \langle p \rangle^m$.

Definition 2.5. Let (\mathbb{Z}_p^m, f) be a linear finite dynamical system, where p is a prime number. Let $\langle p \rangle^m$ be the submodule of \mathbb{Z}_p^m created by m copies of the principal ideal $\langle p \rangle$ in \mathbb{Z}_p . Let

$$\pi: \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^m / \langle p \rangle^m \quad x \mapsto x + \langle p \rangle^m$$

be the natural homomorphism. We say that $\bar{f}: \mathbb{Z}_p^m / \langle p \rangle^m \rightarrow \mathbb{Z}_p^m / \langle p \rangle^m$ defined by $\bar{f}\pi = \pi f$, is the function *induced by the natural homomorphism*, and where

$$\bar{f}(x + \langle p \rangle^m) = f(x) + \langle p \rangle^m$$

for all $x + \langle p \rangle^m \in \mathbb{Z}_p^m / \langle p \rangle^m$.

By *Fitting's Lemma* the state space of a linear system consists of copies of a single tree attached to cycle vertices. In particular, there will always be a copy of this tree in isolation converging to the zero element.

Theorem 2.2 (Fitting's Lemma [BCRO07]). *Let (M, f) be a linear finite dynamical system over commutative ring R . Then there exists a positive integer s and submodules N and T such that*

- (i) $N = f^s(M)$,
- (ii) $T = f^{-s}(0)$,
- (iii) $(M, f) = (N \oplus T, f|_N \oplus f|_T)$,
- (iv) $f|_N$ is invertible,
- (v) $f|_T$ is nilpotent,

where $f|_N$ and $f|_T$ are the restrictions of f to each submodule.

Definition 2.6. Let (M, f) be a linear finite dynamical system over a commutative ring R . Let T be the submodule of M , where for all $t \in T$, $f^k(t) = 0$ for some nonnegative integer k . Then we will say that T forms the *nilpotent component* of the system.

3. PROOF OF THE FUNCTION INDEPENDENT BOUND

In this section we will prove [Theorem A](#), a function independent bound on the height of a linear finite dynamical system of the form (\mathbb{Z}_n^m, f) . The proof is at the end of this section.

Consider linear finite dynamical systems (M, f) where $M = \mathbb{Z}_n^m$. We can derive an upper bound on the height of these systems which is independent of the defining function. By continuing the line of reasoning used in [XZ09] we find the following lemma based on the prime factorization of n .

Lemma 3.1. *Let (\mathbb{Z}_n^m, f) be a linear finite dynamical system and denote by s the height of the system. Then*

$$s \leq m\Omega(n),$$

where $\Omega(n)$ is the number of prime factors of n counting multiplicity.

Proof. By the properties of the linear function every iterated image $f^k(\mathbb{Z}_n^m)$ must be a submodule of the previous iteration. Since a module is an abelian group under addition, each iterated image must also yield an additive subgroup of the previous iteration $f^{k-1}(\mathbb{Z}_n^m)$. By Lagrange's theorem $|f^k(\mathbb{Z}_n^m)|$ divides $|f^{k-1}(\mathbb{Z}_n^m)|$, i.e., the number of elements in the current iteration divides the number of elements in the previous iteration.

Let the prime factorization of n be $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\omega^{\alpha_\omega}$, where ω is the number of distinct prime factors of n . Then the size of the module can be expressed as $n^m = \sum_{i=1}^{\omega} p_i^{m\alpha_i}$. The longest possible chain of proper submodules will be for linear maps, whose iterations reduce in each step the number of elements with a factor of a single prime. This means that the maximum number of iterations s , for a chain of proper submodules is bounded above by

$$s \leq \sum_{i=1}^{\omega} m\alpha_i = m \sum_{i=1}^{\omega} \alpha_i = m\Omega(n),$$

proving the lemma. \square

[Theorem 2.1](#) suggests that the height of a linear finite dynamical system (\mathbb{Z}_n^m, f) , is intimately connected to the possible heights of subsystems modulo p^r , which are derived from the primary decomposition. This is put on firm ground by the following lemma.

Lemma 3.2. *Let (\mathbb{Z}_n^m, f) be a linear finite dynamical system with a defining matrix A over \mathbb{Z}_n . If n has the prime factorization $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\omega^{\alpha_\omega}$, then the height of the system is given by the largest height of*

$$\left\{ (\mathbb{Z}_{p_k^{\alpha_k}}^m, A \bmod p_k^{\alpha_k}) \right\},$$

the collection of subsystems derived from its primary decomposition.

Proof. We want to show that for the product system given in [Theorem 2.1](#), the height is the largest height of the smaller factor systems. The result will then follow from the isomorphism.

The system is isomorphic to a product of subsystems of the form

$$(\mathbb{Z}_{p_k^{\alpha_k}}^m, A \bmod p_k^{\alpha_k}),$$

for each distinct prime factor of n . Let the product set be $X = X_1 \times X_2 \times \cdots \times X_\omega$, where $X_k = \mathbb{Z}_{p_k^{\alpha_k}}^m$. Let \bar{f} be the function of the product system, such that

$$\bar{f}(x_1, x_2, \dots, x_\omega) = (f_1(x_1), f_2(x_2), \dots, f_\omega(x_\omega)),$$

and where each f_k is defined by the matrix $A \bmod p_k^{\alpha_k}$. Let $s_1, s_2, \dots, s_\omega$ be the subsystem heights and let s be the largest one. We have $s \geq s_k$ for each k and according to Fitting's Lemma $f_k^{s+1}(X_k) = f_k^s(X_k)$ for all k . This is now the smallest possible nonnegative integer which settles each subsystem in the product system. Thus s is the smallest nonnegative integer such that $\bar{f}^{s+1}(X) = \bar{f}^s(X)$, which yields s as the system height of the product system. The result follows from the isomorphism. \square

We can now state the proof of the function independent part of the main result.

Proof of Theorem A. By Lemma 3.2, we know that the system height s is given by

$$s = \max \{s_1, s_2, \dots, s_\omega\},$$

where each s_k is the height of a subsystem of the form $(\mathbb{Z}_{p_k}^m, A \bmod p_k^{\alpha_k})$, derived from the primary decomposition. In addition, we know from Lemma 3.1, that each s_k is bounded above by $m\alpha_k$, where α_k is the prime factor exponent of p_k . Hence for each s_k , we have an upper bound $m\alpha_{\max}$, where α_{\max} is the largest exponent in the prime factorization of n . Therefore we also have an upper bound on s given by $m\alpha_{\max}$. \square

4. PROOF OF THE FUNCTION DEPENDENT BOUND

In this section we will prove Theorem B, a function dependent bound on the height of a linear finite dynamical system of the form (\mathbb{Z}_n^m, f) . The proof is at the end of this section.

We will assume that the prime factorization of n is known. By looking at factor subsystems, derived from the primary decomposition, and examining their links to corresponding reduced systems over fields, an upper bound is found for each subsystem. This bound will be function dependent and derived from the reduced system. The main result then follows when considering Lemma 3.2, which states that the system height is given by the largest height of the factor systems. Hence by taking the largest derived bound of all subsystems, we get the result.

We now consider the relation between $(\mathbb{Z}_{p^r}^m, f)$, where p is prime, and a reduced system $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$, where \bar{f} is given in Definition 2.5. Our ultimate goal is to derive from the reduction structural properties and height bounds for the larger system.

We will start with a lemma showing a link between cycle vertices of both systems. This will provide a basis for other results and our understanding of how the state graphs are related.

Lemma 4.1. *Let $(\mathbb{Z}_{p^r}^m, f)$ be a linear finite dynamical system, and let $\langle p \rangle$ be the maximal ideal in \mathbb{Z}_{p^r} . Let \bar{f} be the function induced by the natural homomorphism. Then $x_0 + \langle p \rangle^m$ is a cycle vertex in*

$$(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$$

if and only if the coset contains a cycle vertex in $(\mathbb{Z}_{p^r}^m, f)$.

Proof. We want to show that every cycle vertex $x + \langle p \rangle^m$ in the reduced system, contains, as a coset, a cycle vertex in the larger system. We do this by demonstrating that for every element x in the coset, there exists an element w' in $\langle p \rangle^m$, such that $x + w'$ is a cycle vertex in $(\mathbb{Z}_{p^r}^m, f)$. Conversely, if the coset contains a cycle vertex x_0 such that $f^k(x_0) = x_0$ for some positive integer k , we demonstrate that the properties of the induced function must yield $x + \langle p \rangle^m$ as a cycle vertex in $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$.

(\Rightarrow) Let $x + \langle p \rangle^m$ be a cycle vertex in $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$. Then there exists a $k \geq 1$ such that

$$(\bar{f})^k(x + \langle p \rangle^m) = f^k(x) + \langle p \rangle^m = x + \langle p \rangle^m.$$

Hence $f^k(x) = x + w$ for some $w \in \langle p \rangle^m$. Iterating in multiples of k we get

$$f^{2k}(x) = f^k(f^k(x)) = f^k(x + w) = f^k(x) + f^k(w) = x + w + f^k(w),$$

and in general for positive integers q we have

$$f^{qk}(x) = x + w + f^k(w) + \dots + f^{(q-1)k}(w),$$

by the linearity of the function. We recall that $\langle p \rangle^m$ is a submodule of $\mathbb{Z}_{p^r}^m$, hence

$$w + f^k(w) + \cdots + f^{(q-1)k}(w) = w',$$

for some w' in $\langle p \rangle^m$. Choose integer q such that $qk > h(x)$, where $h(x)$ is the height of x . Then $f^{qk}(x) = x_0$, where x_0 is a cycle vertex in $(\mathbb{Z}_{p^r}^m, f)$. We get

$$x_0 = f^{qk}(x) = x + w',$$

which implies that x_0 is in $x + \langle p \rangle^m$.

(\Leftarrow) Assume $x + \langle p \rangle^m$ contains a cycle vertex x_0 . Then there exists a $k \geq 1$ such that $f^k(x_0) = x_0$. Hence

$$x + \langle p \rangle^m = x_0 + \langle p \rangle^m = f^k(x_0) + \langle p \rangle^m = (\bar{f})^k(x_0 + \langle p \rangle^m) = (\bar{f})^k(x + \langle p \rangle^m),$$

yielding a cycle vertex in $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$. \square

A natural question is how the heights are related for elements of both systems. [Lemma 4.1](#) gives us some information. An element x cannot reach a cycle vertex y in $(\mathbb{Z}_{p^r}^m, f)$ without turning $y + \langle p \rangle^m$ into a cycle vertex in the reduced system. Hence x cannot have a smaller height than $x + \langle p \rangle^m$ in the reduced system. This effectively puts a lower bound on the height of all elements in the coset $x + \langle p \rangle^m$. The following lemma makes it precise.

Lemma 4.2. *Let $(\mathbb{Z}_{p^r}^m, f)$ be a linear finite dynamical system, and let $\langle p \rangle$ be the maximal ideal in \mathbb{Z}_{p^r} . Let \bar{f} be the function induced by the natural homomorphism. If $x + \langle p \rangle^m$ has the height t in*

$$(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f}),$$

then all $y \in x + \langle p \rangle^m$ have heights larger than or equal to t in $(\mathbb{Z}_{p^r}^m, f)$.

Proof. We will do a proof by contradiction. Assume there exists an element y in $x + \langle p \rangle^m$ of height k less than t . Then $f^k(y) = y_0$, where y_0 is some cycle vertex in $(\mathbb{Z}_{p^r}^m, f)$. Therefore, the k th iteration of $x + \langle p \rangle^m$,

$$(\bar{f})^k(x + \langle p \rangle^m) = f^k(x) + \langle p \rangle^m = f^k(y) + \langle p \rangle^m = y_0 + \langle p \rangle^m,$$

contains a cycle vertex and according to [Lemma 4.1](#), the coset must be a cycle vertex. Hence $x + \langle p \rangle^m$ iterates to a cycle vertex in less than t steps. This contradicts the assumption. \square

An immediate consequence of [Lemma 4.2](#) is a lower bound on the height of the larger system by the height of the reduced system.

Corollary. *If t is the height of $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$, then the height s of $(\mathbb{Z}_{p^r}^m, f)$ is bounded below by t .*

Proof. If t is the height of $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$, then there exists an element $x + \langle p \rangle^m$ with this height. By [Lemma 4.2](#) every element of the coset must have a height equal to or larger than t . Hence for the maximal height s of $(\mathbb{Z}_{p^r}^m, f)$ we have $s \geq t$. \square

We now turn our attention to leaf elements. By Fitting's Lemma the system height can be found by the height of the nilpotent component, i.e., there exists a leaf element in the nilpotent component of maximum height. The next two lemmas show that we can deduce properties of $(\mathbb{Z}_{p^r}^m, f)$ by examining leaf elements of the reduced system.

Lemma 4.3. *Let $(\mathbb{Z}_{p^r}^m, f)$ be a linear finite dynamical system, and let $\langle p \rangle$ be the maximal ideal in \mathbb{Z}_{p^r} . Let \bar{f} be the function induced by the natural homomorphism. If $v + \langle p \rangle^m$ is a leaf in*

$$(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f}),$$

then the coset contains only leaf elements in $(\mathbb{Z}_{p^r}^m, f)$.

Proof. We will do a proof by contradiction.

Let $v + \langle p \rangle^m$ be a leaf in $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$. Assume there exists a $y \in v + \langle p \rangle^m$ and an $x \in \mathbb{Z}_{p^r}^m$, such that $f(x) = y$. This implies that

$$\bar{f}(x + \langle p \rangle^m) = f(x) + \langle p \rangle^m = y + \langle p \rangle^m = v + \langle p \rangle^m,$$

contradicting the assumption that $v + \langle p \rangle^m$ is a leaf. \square

Lemma 4.4. *Let $(\mathbb{Z}_{p^r}^m, f)$ be a linear finite dynamical system, and let $\langle p \rangle$ be the maximal ideal in \mathbb{Z}_{p^r} . Let \bar{f} be the function induced by the natural homomorphism. If $v + \langle p \rangle^m$ is a leaf in the nilpotent component of*

$$(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f}),$$

then it contains a leaf in the nilpotent component of $(\mathbb{Z}_{p^r}^m, f)$.

Proof. Let $v + \langle p \rangle^m$ be a leaf of height t in the nilpotent component of $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$. Then

$$(\bar{f})^t(v + \langle p \rangle^m) = f^t(v) + \langle p \rangle^m = \langle p \rangle^m,$$

therefore t is the smallest positive integer such that $f^t(v) = w$, for some $w \in \langle p \rangle^m$. According to Lemma 4.3, every $y \in v + \langle p \rangle^m$ is a leaf, and by the corollary of Lemma 4.2, the height s of $(\mathbb{Z}_{p^r}^m, f)$ is bounded from below by t .

Since $\langle p \rangle^m$ is a submodule, $f^k(w)$ is an element in $\langle p \rangle^m$ for all $w \in \langle p \rangle^m$ and positive integers k . Therefore, given a system height of s , $f^s(v) = w_0$, where w_0 is some cycle vertex in $\langle p \rangle^m$.

If w_0 is of period l , i.e., $f^l(w_0) = w_0$, we choose an integer q such that $r = ql - s$ is nonnegative. Then $y = v - f^r(w_0) = v - w'$, is in $v + \langle p \rangle^m$, and

$$f^s(y) = f^s(v - w') = f^s(v) - f^s(f^{ql-s}(w_0)) = w_0 - w_0 = 0,$$

proving the lemma. \square

In dealing with the relevant reduced subsystems of $(\mathbb{Z}_{p^r}^m, f)$, it is handy to work with isomorphic systems. The next proposition shows that the induced functions have simple representations based on the matrix of the linear function.

Proposition 4.5. *Let $(\mathbb{Z}_{p^r}^m, f)$ be a linear finite dynamical system with a defining matrix A over \mathbb{Z}_{p^r} . Let $\langle p \rangle$ be the maximal ideal in \mathbb{Z}_{p^r} and let \bar{f} be the function induced by the natural projective homomorphism. Then $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$ is isomorphic to $(\mathbb{Z}_p^m, A \bmod p)$, and $(\langle p \rangle^m, f)$ is isomorphic to $(\mathbb{Z}_{p^{r-1}}^m, A \bmod p^{r-1})$.*

Proof. The proof is a simple examination of induced functions of bijective morphisms between systems.

Consider $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$. Let $\pi: \mathbb{Z}_{p^r}^m \rightarrow \mathbb{Z}_{p^r}^m / \langle p \rangle^m$ be the natural homomorphism, where

$$\pi(x) = x + \langle p \rangle^m = x \bmod p + \langle p \rangle^m,$$

for all $x \in \mathbb{Z}_{p^r}^m$. We may express the induced function \bar{f} of $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$ by

$$\bar{f}(x + \langle p \rangle^m) = f(x) + \langle p \rangle^m = (Ax) \bmod p + \langle p \rangle^m,$$

for all $x + \langle p \rangle^m$. Consider the bijection

$$\psi: \mathbb{Z}_{p^r}^m / \langle p \rangle^m \rightarrow \mathbb{Z}_p^m \quad x + \langle p \rangle^m \mapsto x \bmod p,$$

which we take as a morphism between systems $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$ and $(\mathbb{Z}_p^m, \bar{g})$. Here we have an induced function

$$\bar{g}: \mathbb{Z}_p^m \rightarrow \mathbb{Z}_p^m \quad \bar{g}(x) = \psi \bar{f} \psi^{-1}(x) = Ax \bmod p,$$

for all $x \in \mathbb{Z}_p^m$, and therefore ψ acts as an isomorphism between $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$ and $(\mathbb{Z}_p^m, A \bmod p)$.

Consider $(\langle p \rangle^m, f)$. Here every element $w \in \langle p \rangle^m$ can be represented uniquely by pv for some element $v \in \mathbb{Z}_{p^{r-1}}^m$. Hence there exists a bijection $\phi : \langle p \rangle^m \rightarrow \mathbb{Z}_{p^{r-1}}^m$, by

$$\phi(pv) = v,$$

which induces a function $g(v) = \phi f \phi^{-1} = \phi(Apv) = Av \bmod p^{r-1}$. As such, $(\langle p \rangle^m, f)$ is isomorphic to $(\mathbb{Z}_{p^{r-1}}^m, A \bmod p^{r-1})$. \square

The next lemma shows, that it is possible to put a lower and upper bound on the height of (\mathbb{Z}_p^m, A) by the height of the reduced system $(\mathbb{Z}_p^m, A \bmod p)$.

Lemma 4.6. *Let $(\mathbb{Z}_{p^r}^m, f)$ be a linear finite dynamical system with a defining matrix A over \mathbb{Z}_{p^r} . Let s be the height of the system. Then*

$$s_1 \leq s \leq rs_1,$$

where s_1 is the height of the system $(\mathbb{Z}_p^m, A \bmod p)$.

Proof. Let z be a leaf of maximal height s in the nilpotent component of $(\mathbb{Z}_{p^r}^m, f)$. Since

$$f^s(z) + \langle p \rangle^m = 0 + \langle p \rangle^m = \langle p \rangle^m,$$

$z + \langle p \rangle^m$ is a coset in the nilpotent component of $(\mathbb{Z}_{p^r}^m / \langle p \rangle^m, \bar{f})$. As such z reaches $\langle p \rangle^m$ within t iterations, where t is the system height of the reduced system. Assuming maximal height, the reached element w within $\langle p \rangle^m$ is of system height k of $(\langle p \rangle^m, f)$. Hence s is bounded by $t \leq s \leq t + k$.

Working instead in the isomorphic systems of [Proposition 4.5](#), and denoting by s_k the height of systems of the form $(\mathbb{Z}_{p^k}^m, A \bmod p^k)$, we have $t = s_1$, $k = s_{r-1}$ and $s = s_r$. Hence by recursion

$$s_1 \leq s_r \leq s_1 + s_{r-1} \leq 2s_1 + s_{r-2} \leq \dots \leq rs_1,$$

proving the lemma. \square

We are now ready to state the proof of the function dependent part of the main result.

Proof of Theorem B. As we know from [Lemma 3.2](#), the height is determined by the largest height of factor systems in the primary decomposition. Applying [Lemma 4.6](#) to each such factor system and taking the largest bound yields the result.

Let $h_i, i = 1, 2, \dots, \omega$ be the heights of the factor subsystems $(\mathbb{Z}_{p_i}^{m_{\alpha_i}}, A \bmod p_i^{\alpha_i})$ derived from the primary decomposition. According to [Lemma 4.6](#) each $h_i \leq \alpha_i s_i$, where s_i is the height of $(\mathbb{Z}_{p_i}^m, A \bmod p_i)$. Thus for all i , $h_i \leq \alpha_k s_k$, for some maximum product $\alpha_k s_k$ in

$$\{\alpha_1 s_1, \alpha_2 s_2, \dots, \alpha_\omega s_\omega\},$$

therefore we have a system height s bounded by $\alpha_k s_k$ according to [Lemma 3.2](#). \square

Remark 4.1. Given the system (\mathbb{Z}_n^m, f) , we consider the largest product αs , where α is an exponent of some prime p in the factorization of n , and where s is the height of the system mod p . The function independent bound of [Theorem A](#) yields a bound $\alpha_{\max} m$, where α_{\max} is the largest of all exponents in the prime factorization. Since $\alpha \leq \alpha_{\max}$ and $s \leq m$, [Theorem B](#) offers the sharpest bound in this article. \spadesuit

REFERENCES

- [BCRO07] Dorothy Bollman, Omar Colón-Reyes, and Edusmildo Orozco. “Fixed points in discrete models for regulatory genetic networks”. In: *EURASIP Journal on Bioinformatics and Systems Biology* 2007 (2007).
- [CRJL06] Omar Colón-Reyes, Abdul Salam Jarrah, and Reinhard Laubenbacher. “Monomial Dynamical Systems over Finite Fields”. In: *Complex Systems* 16 (2006), pp. 333–342.
- [CRLP05] Omar Colón-Reyes, Reinhard Laubenbacher, and Bodo Pareigis. “Boolean monomial dynamical systems”. In: *Annals of Combinatorics* 8.4 (2005), pp. 425–439.
- [Den15] Guixin Deng. “Cycles of linear dynamical systems over finite local rings”. In: *Journal of Algebra* 433 (2015), pp. 243–261.
- [HT05] René A Hernández Toledo. “Linear finite dynamical systems”. In: *Communications in Algebra* 33.9 (2005), pp. 2977–2989.
- [LS04] Reinhard Laubenbacher and Brandilyn Stigler. “A computational algebra approach to the reverse engineering of gene regulatory networks”. In: *Journal of theoretical biology* 229.4 (2004), pp. 523–537.
- [LT94] Dan Laksov and Anders Thorup. “Counting matrices with coordinates in finite fields and of fixed rank”. In: *Mathematica Scandinavica* (1994), pp. 19–33.
- [VZGG13] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge university press, 2013.
- [XZ09] Guangwu Xu and Yi Ming Zou. “Linear dynamical systems over finite rings”. In: *Journal of Algebra* 321.8 (2009), pp. 2149–2155.